Cisco ASA Shun-functie configureren om virtuele apparaten vrij te stellen

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Cisco ASA configureert om het virtuele toestel vrij te stellen van de component voor bedreigingsdetectie. De Cisco ASA-component voor bedreigingsdetectie voert pakketinspecties uit op DNS en andere protocollen. Umbrella Support raadt deze wijzigingen in de ASA-configuratie aan om te voorkomen dat deze functie in strijd is met onze virtuele toepassing:

- Stel het virtuele toestel vrij van de functie 'shun' voor de detectie van bedreigingen, zoals beschreven in dit artikel.
- Vrijstelling van de Virtual Appliance van DNS-pakketinspectie om onze DNS-codering (DNScrypt) mogelijk te maken, die in dit artikel wordt behandeld: Cisco ASA Firewall blokkeert DNScrypt.

Threat Detection 'Shun'-functie

Wanneer de functie 'Shun' is ingeschakeld, kan de ASA een IP-adres van de bron volledig blokkeren dat detectieregels voor bedreigingen activeert. Meer details zijn te vinden in het Cisco-artikel: ASA Threat Detection Functionality and Configuration.

De Virtual Appliance stuurt normaal gesproken een zeer groot aantal DNS-query's naar Umbrella DNS-resolvers. In gevallen waarin er een lokaal probleem is met de verbinding met de resolvers (zoals een tijdelijke netwerkonderbreking/latentie) kunnen deze query's mislukken. Vanwege het enorme volume aan query's dat wordt verzonden, zorgt zelfs een klein percentage dat faalt ervoor dat de ASA de Virtual Appliance mijdt; wat leidt tot een volledige DNS-uitval voor een bepaalde periode.

Het virtuele toestel vrijstellen

Opmerking: de opdrachten in dit artikel zijn alleen bedoeld als richtlijn en het wordt aanbevolen om een Cisco-expert te raadplegen voordat u wijzigingen aanbrengt in een productieomgeving.

Via CLI:

- Voer de volgende opdracht uit om te voorkomen dat het IP-adres van het toestel wordt genegeerd: **no shun**

Via ASDM-interface:

- Kies het deelvenster Configuratie > Firewall > Dreigingsdetectie.
- Als u wilt voorkomen dat het IP-adres van het toestel wordt gemeden, voert u een adres in het veld 'Netwerken uitgesloten van schuwen' in. U kunt meerdere adressen of subnetten invoeren, gescheiden door komma's.

Bepaal of het apparaat is 'gemeden'

Als deze stappen niet zijn gevolgd, kan het apparaat in sommige omstandigheden worden 'gemeden', wat leidt tot een DNS-storing.

Wanneer het virtuele toestel geen externe connectiviteit heeft, registreert de Cisco ASA-console de gebeurtenis als volgt:

4|06 jun 2014 14:00:42|401004: Gemoed pakket: 192.168.1.3 ==> 208.67.222.222 op interface binnen
4|06 jun 2014 14:00:42|401004: Gemoed pakket: 192.168.1.3 ==> 208.67.222.222 op interface binnen

Als u een lijst met momenteel gemeden IP-adressen wilt zien, voert u deze opdracht uit op de ASA: **show shun**

Voer deze opdracht uit op de ASA om de momenteel gemeden IP-adressen onmiddellijk te wissen: **clear shun**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.